International Journal of Communication Networks and Information Security
2024, 16(4)
ISSN: 2073-607X,2076-0930
https://ijcnis.org/

Research Article

Detection Protocol for the Five Variants of Selective Forwarding Attack in the Internet of Things

Diédié Gokou Hervé Fabrice [1*], Tchimou N'Takpé[2]

[1]Université Peleforo Gon Coulibaly, Korhogo, Ivory Coast
[2]Université NanguiAbrogoua, Abidjan, Ivory Coast

***Corresponding Author:**herve.diedie@upgc.edu.ci

Citation: Diédié Gokou Hervé Fabrice, Tchimou N'Takpé "Detection Protocol for the Five Variants of Selective Forwarding Attack in the Internet of Things" *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 16, no 4,2024. pp. yyy, xx. xxx.

ARTICLE INFO

Received: 1 Sep 2024
Accepted: 11 Oct 2024

ABSTRACT

RPL (Routing Protocol for Low power and lossy networks), the most widely used routing protocol in the Internet of Things, has numerous security vulnerabilities. These make it particularly susceptible to selective forwarding attacks. This work aims to add a scalable, fast, and accurate detection process to RPL for the five variants of this attack, regardless of the type of data collected. To this end, each node is constantly evaluated by its neighbors. Packets routing is modeled as a maximum flow problem, which allows for the prediction of maximum throughput and average delivery delay. By comparing these indicators to the node's actual performance, each neighbor estimates a trust level. The node's final status is determined through feedback from the neighbors, following an approach inspired by Dempster-Shafer theory. Simulation showed thattheproposed scheme is precise, energy-efficient, and outperforms similar recent state-of-the-art contributions.

Keywords: IoT, SFA, RPL, Security

INTRODUCTION

The Internet of Things (IoT) refers to a set of technologies enabling the interconnection of various smart electronic devices [1].Applications of IoT are found in fields such as home automation, defense, transportation, healthcare, and industry [2]. The performance of these networks largely depends on their routing protocols, the most popularis RPL (Routing Protocol for Low-Power and Lossy Networks). Created by the IETF (Internet Engineering Task Force), RPL includes several security mechanisms aimed at ensuring the resilience of the underlying network. However, it has certain vulnerabilities that expose the infrastructures using it to numerous attacks [3] – [5].

The Selective Forwarding Attack (SFA) is one of the most insidious [6]; it leads an infected machine to randomly drop the data it is supposed to forward, thereby degrading the quality of service. The resulting packet loss rates are typically low, making this anomaly difficult to detect. Moreover, there are currently five different variants of this attack [7]. Most solutions in the literature use methods for calculating the trust level of nodes based solely on the number of lost packets.Additionally, these solutions often leverage two processes to establish or refute the status of any suspected node. This scheme contributes to increased latency and energy consumption. Furthermore, these solutions often use techniques that struggle to apply equally to the five known variants ofSFA. The present work aims to address these shortcomings.

We propose a fully distributed strategy where calculating the trust level of nodes considers not only the number of forwarded packets but also the residual energy and transmission delay. When there are multiple opinions about a node given by its neighbors, a process based on Dempster-Shafer's theory is applied to establish

the final status of the suspected node.

The main contributions of this work are as follows:

- A trust level estimation process for nodes modeled as a maximum flow problem.
- Implementation of a fully distributed model for detecting and neutralizing malicious nodes.
- effective strategy applicable simultaneously tothe five known variants of SFA.

The remainder of this article is organized as follows. Section 2 presents the major works recently proposed in the literature. In Section 3, we detail our proposal. Section 4 describes the experimental framework used to evaluate its performance. The results obtained are analyzed and discussed in Section 5. Finally, Section 6 concludes the work.

LITERATUREREVIEW

For data forwarding, RPL constructs a tree denoted as a DODAG (Destination Oriented Directed Acyclic Graph), with the destination node as the root. The root node is responsible for storing and discovering routing paths. RPL allowsthe creation of multiple instances of a DODAG with the same root. Similarly, other nodes can belong to one or more DODAGs. These have a hierarchical structure, so a parent-child relationship exists between the nodes within these trees. To construct and maintain DODAGs, RPL uses four main types of control messages: DIO (DODAG Information Object), DIS (DODAG Information Solicitation), DAO (DODAG Advertisement Object) [3], [4]. DIO is the most frequently used message. The latter is sent by the root to all the other nodes to announce the network structures that help discover, create, and maintain DODAGs. Additionally, DODAGshelp to quicklyannounce detection results, while avoiding the overhead associated with messages used for anomaly reporting.

RPL has both internal local and global security mechanisms. They are activated after any change in the topology, such as the disappearance of a link or a node. However, these basic mechanisms struggle to cope with the ever-growing and increasingly sophisticated threats. This has led to numerous studies aimed at enabling RPL to withstand various attacks, including the one known asSFA (Selective Forwarding Attack)[3], [6], [8], [9]. The objective is to compromise the routing paths discovered so far. To avoid detection, the compromised node may, for example, prefer to drop data packets instead of control messages belonging to the protocol. This attack as currently has five known variants.

The first variant, called SFA-I or SV-SFA (Selective Victim SFA), involves randomly or non-randomly selecting victims from which to attack the system.

The second one, or SFA-II, often referred to as Neglect and Greed, causes the attacking node to forward control messages (DIS, DIO, DAO, and DAOACK) and its own packets while destroying the data packets of other nodes.

The third one, named SFA-III, leads the attacked node to reroute data packets to an inappropriate path.

The fourth one, known as SFA-IV,makes the node createconfused routing information between nodes by delaying the received packets.

The fifth one, called SFA-V, is the most recent known variant. It was introduced by Jiang and Liu [10]. Malicious nodes dynamically adjust the packet transfer rate based on the network's state. Additionally, a malicious node can arbitrarily choose one or more child nodes and drop the packets destined for them.

Several approaches exist for detecting a Selective Forwarding Attack (SFA). These are generally classified based on various criteria, such as metrics related to node behavior (loss rate, latency, throughput, etc.) [11]. Among these approaches, we can mention trust-based approaches [12], [13].

In a network, trust is generally defined as a relationship between entities regarding the reliability and scalability of their communication. It is based on the previous interactions and behavior of the nodes. The cumulative value obtained for a node represents its reputation in the network. This trust level granted to the node will be used by its direct neighbors for creating various logical topologies.In this category, solutions can be classified according to the technique used to aggregate the trust level attributed to each node. These refer to the accumulation of trust evidence collected by the node itself or by its neighbors. The main aggregation techniques include weighted sum, belief theory, Bayesian inference (with belief updating), fuzzy logic, and regression analysis [14]. It should be noted that the concepts of reputation and trust are generally associated with belief and even

considered synonyms [15]. However, some authors argue that trust is active, whereas reputation is a passive concept [16]. In recent years, numerous trust-based solutions have been proposed in the literature [7]. They are in the majority of the work found in the literature [3]. In this section, we review the most recent leading solutions.

Pantel and Jinwala [17] suggest a reputation-based approach. Nodes' reputation is evaluated by comparing the actual packet loss rate with an estimated rate. The result obtained is considered in the selection of parent nodes. The probability of packet loss is expressed using the binomial distribution. However, this approach does not account for all the variants of SFA, particularly the fifth one.

Ribera *et al.* [18] propose a precise and efficient detection of various types of routing and DoS(Denial of Service) attacks, including SFA. To achieve this, a hybrid detection strategy is implemented by the central module. This strategy is based on the signatures and specifications of anomalies. The solution uses a heart-beat type protocol as a detection method. However, no specific approach is proposed for the different variants of SFA.

Yaman *et al.* [19] suggest a strategy that incorporates a packet drop time by the attacker and a service period for trusted mobile nodes deemed reliable. However, such a strategy struggles to scale.

Jiang and Liu [10] propose a trust-based solution consisting of three modules. The detection module analyzes the trust level of each node based on the data packets received. The notification module encapsulates this information into DIO messages before sending them to all the other nodes. The isolation module identifies the children of malicious nodes, potentially forcing them to select new parents based on the received DIO messages. To prevent attacks in which malicious nodes temporarily adopt good behavior to increase their trust level, a counter is used to observe the nodes' behavior in forwarding packets over a long period.

More recently, Alansari *et al.* [20] presented a four-layer detection approach designed for a context involving node mobility. The first layer collects three types of information from all immediate neighbors through three sub-layers, each related to control packet information, data packet information, and the overall packet information. The second layer calculates three trust levels: the one related to the successful routing of all packets, the trust level for control packet routing, and the trust level related to data packet routing. The third layer handles decision-making after calculating the various trust levels. A penalty is imposed on a node if its trust level falls below a threshold. However, forgiveness is granted, considering the possibility that the penalized node may not be the actual attacker. The fourth layer, known as the backup and restoration layer, is activated when nodes loose essential data due to some failure. After the backup period expires, the node transmits the IP address and tolerance level applied to the nodes that were blocked since the previous backup. This strategy allows the protocol to monitor traffic and node behavior to evaluate their actions within the network. Despite its innovative aspect, this solution introduces protocol overhead, leading to significant energy losses. Additionally, it struggles to address all SFA variants, especially the fifth one.

METHODOLOGY

In this section, we present our solution for detecting the different variants of SFA. It is named FLT-RPL (Flow Link and Trust-based RPL). We first describe our model for estimating the trust level of nodes, then we detail the processes for identifying and neutralizing malicious nodes.

Motivation and Objectives

Many existing works in the literature are centralized, which limits their application to sparse networks. Indeed, node behavior monitoring, the evaluation, and the propagation of their trust level are often entrusted to a central entity, namely the root nodeassuming that the latter cannot be attacked. Moreover, these works do not consider all the known variants of the Selective Forwarding Attack (SFA), particularly the fifth one. It is therefore necessary to propose a fast, scalable, energy-efficient, and fully distributed solution. Above all, this solution must be able to address equally all the known variants of SFA.

Estimation of Nodes' Trust Level

Each node has a sub-layer responsible for monitoring its energy activity over a given period, counting the packets received and forwarded, as well as estimating the quality of links with its neighbors. The duration Δt of this period is set as a parameter.

After Δtseconds each node decides to measure the trust to be granted to the nodes in its 2-hop neighborhood from its parent and vice versa from its children. In the remainder of this paper these two neighborhoods will be

referred to as the *2-parent neighborhood* and the *2-children neighborhood*, while the node wishing to evaluate the trust of its neighbors will be called the *inquiring node*.

Let G be the graph induced by the sub-network representing the 2-parent neighborhood or the 2-children neighborhood on the DODAG of an inquiring node . We have $G = (V \cup \{s, t\}, E, C)$, where V denotes the set of nodes in this sub-network; $s$and t are two fictitious nodes representing, respectively, a fictitious data source related to the inquiring node and a sink representing the nodes that are 3 hops away; that is, the neighbors of the nodes with the highest ranks in this sub-network. E is the set of arcs connecting the various nodes; in other words, $E = \{ (i,j) | i,j \in V\}$, and C is a function from E into $\mathbb{R}$ with C_{ij} denoting the capacity of the arc (i,j).

Let $\Gamma(i)$ and $\Gamma^{-1}(i)$represent respectively the set of successors and the set of predecessors of node i on G.

Let ϕ_{ij}be the data flow transmitted from node i to node j. The amount of the data sent from i to j will be referred to as a flow.

Thus, to calculate the maximum flow ϕ^* that should have exited from the nodes with the highest rank, the inquiring node must solve the following linear program:

$$\text{Max} \sum_{j \in \Gamma^{-1}(t)} \phi_{jt} \quad (1)$$

$$\text{St}: \ \phi_{ij} \leq C_{ij} \ , \ \forall (i,j) \in E \quad (2)$$

$$\sum_{j \in \Gamma(i)} \phi_{ij} = \sum_{j \in \Gamma^{-1}(i)} \phi_{ji} \ , \ \forall i \neq s,t \quad (3)$$

$$\phi_{ij} \geq 0 \ , \ \forall (i,j) \in E \quad (4)$$

Equation (1) expresses the objective, namely, to determine the total maximum flow that should traverse the sub-network; in other words, the flow arriving at the sink t. Constraint (2) specifies that the flow passing through each arc cannot exceed its capacity. Constraint (3) requires that the amount of flow entering each node i is equal to the amount of flow leaving it. Constraint (4) states that each flow considered is positive.

$$C_{ij} = \frac{\xi_i^{(t-1)}}{Er_{ij}} \quad (5)$$

The capacity C_{ij} of an arc (i,j) is estimated using Equation (5), where $\xi_j^{(t-1)}$andEr_{ij} denote, respectively, the residual energy of node $j$after the last inspection and the amount of energy lost by this node after receiving a packet via the arc(i,j). Note that Er_{ij} is estimated using the underlying energy model.

D_{ij} of an arc $(i,j)$is estimated using Equation (6), where W_{ij} and $SINR_{ij}$ represent the bandwidth and the signal-to-interference-plus-noise ratio measured on this arc, respectively.

$$D_{ij} = W_{ij} \times \log_2\left(1 + SINR_{ij}\right) \quad (6)$$

Let C_{ij} denote the number of packets that node j can receive, considering its residual energy, while D_{ij} represents the number of bits that node i is able to send to it per second, given the current state of the radio link between them.

Note that, as is customary in solving this problem, before starting the process, each leaf (node with the lowest rank) f, including the inquiring node, will be connected to the fictitious source s such that the flow ϕ_{sf}represents the number of packets that f claims to have forwarded.

Solving the aforementioned program will allow the inquiring node$k$ to determine the number of packets ϕ_{ij} that each node i was supposed to forward to its neighbor j, based on the information provided regarding node j's reception capacity $C_{ij}$and node$i$'s transmission capacity D_{ij}over the link(i,j). Using Equation (7), it can then deduce $\hat{\xi}_{ki}^{(t)}$the current residual energy that each node i should theoretically have, in the worst-case scenario.

$\Gamma_k(i)$and $\Gamma_k^{-1}(i)$represent the set of successors and predecessors, respectively, of node$i$ in the neighborhood of k. η denotes the number of transmission attempts before giving up.

$$\hat{\xi}_{ki}^{(t)} = \xi_i^{(t-1)} - \left(\left(\sum_{j \in \Gamma_k^{-1}(i)} \phi_{ji} \times Er_{ji} \right) + \left(\sum_{j \in \Gamma_k(i)} \phi_{ij} \times \eta \times Et_{ij} \right) \right) \quad (7)$$

Once $\hat{\xi}_{ki}^{(t)}$ is determined, the inquiring node k can estimate, using Equation (8), the trust levelto assign to each neighbor i.

$$\delta_{ki}^{(t)} = \left| 1 - \frac{\left| \xi_i^{(t)} - \hat{\xi}_{ki}^{(t)} \right|}{\xi_i^{(t)}} \right| \quad (8)$$

Detection and Elimination of Malicious Nodes

After calculating the trust level $\delta_{ki}^{(t)}$, if it is less than 0.5, neighbor i is considered malicious by the inquiring node k.

After the investigation process, the inquiring node's notification moduleencapsulates the results in the DIO messages and sends them to all the nodes in its DODAG. Consequently, if within the same period a node receives multiple reports concerning a neighbor$i$ from different inquiring nodes, it uses a method inspired by Dempster-Shafer belief theory [22] to resolve the uncertainty. It should be noted that these reports may include the inquiring node $k$itself if it has just carried out an investigation involving this neighbor$i$.

Let Ω be a set of n propositions denoted $p_1, p_2, \dots, p_n$. $\Omega = \{p_1, p_2, \dots, p_n\}$ is called a frame of discernment, and $2^\Omega = \{\emptyset, \{p_1\}, \dots, \{p_n\}, \{p_1, p_2\} \dots, \Omega\}\}$ is its power set. Similarly, a mass belief function, denoted$m$, is defined as a mapping from 2^Ω to [0,1] such that $m(\emptyset) = 0$ et $\sum_{A \in 2^\Omega} m(A) = 1$. Thus, $m_k(A)$ quantifies the mass of belief allocated by source$k$ to the subset A ofΩ. The Belief function is denoted by $Bel(.)$and the Plausibility function by $Pl(.)$. For a source k, these two functions are calculated via Equations (9) and (10), respectively.

$$Bel_k(A) = \sum_{B \in 2^\Omega : (B \subseteq A) \neq \emptyset} m_k(B) \quad (9)$$

$$Pl_k(A) = \sum_{B \in 2^\Omega : (B \cap A) \neq \emptyset} m_k(B) = 1 - Bel_k(\bar{A}) \quad (10)$$

$[Bel_k(A), Pl_k(A)]$ represents the uncertainty with respect to source k. Thus, two mass functions m_k and $m_l$arising from the same frame of discernment and belonging to two independent sources can be combined using the Dempster combination rule, as expressed by Equations (11) and (12).

$$m_k(A) \oplus m_l(A) = \begin{cases} 0 \text{ if } A = \emptyset \\ \dfrac{1}{1-K} \displaystyle\sum_{(B \cap C) = A} m_k(B) m_l(C), \text{ otherwise} \end{cases} \quad (11)$$

$$K = \sum_{(B \cap C) = A} m_k(B) m_l(C) \quad (12)$$

Unfortunately, this combination method can become complex, especially when $|\Omega|$ is large. Reducing this complexity is an open question [22][23].

In our context, we propose to use the approach based on the NTU (New Total Uncertainty) indicator inspired by Liu *et al.* [23], with$|\Omega| = 2$. Indeed, we only have two possible propositions p_1 and p_2, namely "the neighbor is malicious" and "the neighbor is normal," within the frame of discernment. Let $|I|$represent the number of sources,

where I denotes the set of inquiring nodes that have issued reports concerning the neighbor in question. Equation (13) helps calculate the$NTU(m_k)$of each inquiring node k.

Note that $\forall\, k \in I$, we have $m_k(\{p_1\}) = \delta_{ki}^{(t)}$, $m_k(\{p_2\}) = 1 - \delta_{ki}^{(t)}$et $m_k(\{p_1, p_2\}) = 0$.

$$NTU(m_k) = \frac{1}{|\Omega|}\sum_{i=1}^{|\Omega|}\left(\frac{2}{1 + d_E([Bel_k(\{p_i\}), Pl_k(\{p_i\})], [0,1])}\right) - 1 \qquad (13)$$

With d_E representing the Euclidean distance obtained from Equation (14), $Bel_k(.)$ and $Pl_k(.)$ are calculated respectively using Equations (9) and (10).

$$d_E([Bel_k(\{p_i\}), Pl_k(\{p_i\})], [0,1]) = \sqrt{[Bel_k(\{p_i\}) - 0]^2 - [Pl_k(\{p_i\}) - 1]^2} \qquad (14)$$

$$\forall i \in (1, \dots, |\Omega|) \quad \widetilde{m}(\{p_i\}) = \sum_{k \in I} m_k(\{p_i\})\, \omega(m_k) \qquad (15)$$

Equation (15) helps obtaining the weighted average of each mass function, with $\omega(m_k)$ being the weight calculated using Equation (16).

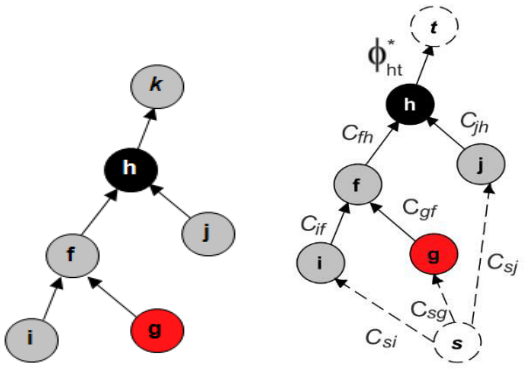
$$\omega(m_k) = \frac{NTU(m_k)}{\sum_{l \in I} NTU(m_l)} \qquad (16)$$

$$\forall i \in (1, \dots, |\Omega|) \qquad \widehat{m}(\{p_i\}) = \oplus_{k \in I}\, \widetilde{m}_k(\{p_i\}) \qquad (17)$$

$$i^* = \underset{i \in (1,\dots,|\Omega|)}{\operatorname{argmax}}\, \widehat{m}(\{p_i\}) \qquad (18)$$

$p_i$is obtained using Equations (17) and (18) then the opinion to be retained regarding the neighbor. More concretely, in our context, if $\widehat{m}(p_1) > \widehat{m}(p_2)$, then the neighbor is considered malicious; otherwise, the neighbor is said normal.Once a malicious node is duly identified, its neighbors can isolate it and reselect their new parents based on the DIO messages received. After executing this process, the malicious nodes become isolated from the others and are thus neutralized.

In Figure 1-a), node g is the inquiring node wishing to assess the trust level of node g, which is in its two-hop neighborhood. Node g collects information regarding the forwarding activities from$h$'s children (nodes f and j), and then from its sibling i (via its parent f). Node $g$can then construct the packet forwarding graph described in Figure 1-b) by adding to the leaves (nodes without children) the fictitious source$s$, and to the evaluated node$h$, a fictitious sink$t$, which is actually h's parent.



a) *b)*

Figure 1- Finding the maximum flow: a) on the graph induced by the neighborhood of the inquiring node g; b) on a resulting graph with the fictitious source node s and sink node t.

Algorithm 1 describes the inspection processes used by each node to detect and potentially eliminate malicious neighbors.

Algorithm 1 Detection andelimination of malicious nodes

Input: neighbor table, Δt

Output: neighbor table updated

1: chooseanew 2-hop neighborhood

2: collect dataabout this neighborhood

3: buildthe graph induced by this neighborhood

4: find maximal flowonthis graph e.g.using Ford-Fulkerson algorithm Eqs. (1) – (6)

5: **for each**neighboron this graph

6: getitstheorical residual energyfromin and out flows Eq. (7)

7: estimate itstrust level via itsactual residual energy Eq. (8)

8: **endfor**

9: send this trust level to the 2-hopneighbors

10: **for each**neighboron this graph

11: **if**located1-hop away

12: **if** othertrust levelsaboutthis neighbor are received

13: decideits statususing Dempster-Schafer methodEqs. (9) - (18)

14: **else**

15: directlyits status (maliciousif level<0.5 andnormal otherwise)

16: **end if**

17: ifits status is maliciousremove this neighbor fromthe table

18: **end if**

19: **end for**

9:

2 randomly choose next inquiry date in [now ,now +Δt]

0:

PERFORMANCEEVALUATION

To evaluate the performance of FLT-RPL, we conducted various experiments on networks created using the Contiki/Cooja 3.0 simulator [24]. This evaluation focused on three criteria: decision quality, latency (delay), and energy efficiency.

The results are compared with those obtained from two major protocols recently proposed in the literature: RPLAD3 by Alansari *et al.* [20] and the solution proposed by Jiang and Liu [10], referred to as JL-RPL.

Table 1 summarizes the parameters used during the experiments.

Table 1 : Simulation parameters.

Parameter	Value
Deployment area	130 m X 130 m
Deployment mode	Random
Node type	TMote Sky
Initial energy	3 J
Numberof nodes	10 - 100
Malicious nodes ratio	10%
Node range	50 m
Transport layer protocol	UDP
Network layer protocol	IPv6
MAC layer protocol	ContikiMAC
Number of sending trialsη	4
Routing protocol	RPL)
Timebetweentwo inspectionsΔt	5s
Interference range	100 m
Packet size	46 octets
Data production period	0,1 ms
Link failure model	UDGM-distance loss
Experiment duration	1h
Warm-Up	10 mn

Quality of Decision

To study the decision quality of the three protocols, we randomly deployed 10 networks, varying the node population from 10 to 100 in increments of 10, with 10% of the nodes being malicious for each of the 5 variants of SFA. These malicious nodes were selected randomly and uniformly. Each experiment was repeated 35 times and lasted 1 hour. At the end of each experiment, the numbers of False Positives (FP), True Positives (TP), True Negatives (TN), and False Negatives (FN) were determined. The averages of these values were calculated for each type of experiment with a 95% confidence interval. These values were then used to compute well-known indicators from the literature: Precision, Accuracy, Sensitivity (Recall), and Specificity obtained via Equations (19) – (22).

$$Precision = \frac{TP}{TP + FP} \tag{19}$$

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{20}$$

$$Sensitivity = \frac{TP}{TP + FN} \tag{21}$$

$$Specificity = \frac{TN}{TN + FP} \tag{22}$$

Delay

To evaluate the latency of the three protocols in detecting a malicious node, we randomly deployed 10 networks under the conditions described in Section 4.1. The experiment ended as soon as a True Positive was detected. Each experiment was repeated 35 times. After each experiment, the elapsed time was measured. Thevalues were averagedandcalculated for each type of experiment, with a 95% confidence interval.

Energy efficiency

To assess the energy cost of the detection process for each protocol, we randomly deployed 10 networks under the conditions described in Section 4.1. The experiment ended as soon as a True Positive was detected. Each experiment was repeated 35 times. At the end of each experiment, the residual energy of each node was measured and then compared to its initial energy. An average for the entire network was determined. The 35 values obtained were averagedandcalculated for each type of experiment, with a 95% confidence interval.

RESULTSAND DISCUSSION

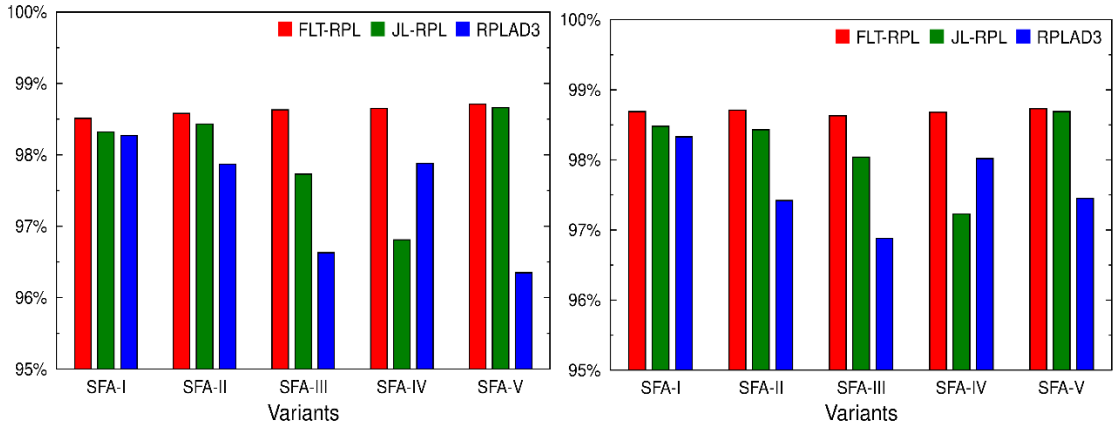
In this section, we present, analyze, and discuss the results of the experiments conducted under the previously described conditions.

Quality of Decision

Figure 2-a) shows the results of evaluating of the precision of the decisions made regarding each of the5 variants of SFA for a population of 100 nodes. It is noted that all three protocols achieve values above 95%. However, FLT-RPL produces the best results. This is attributed to its trust evaluation strategy, which is focused not only on the number of packets, unlike the two other protocols. In fact, FLT-RPL additionally considers the

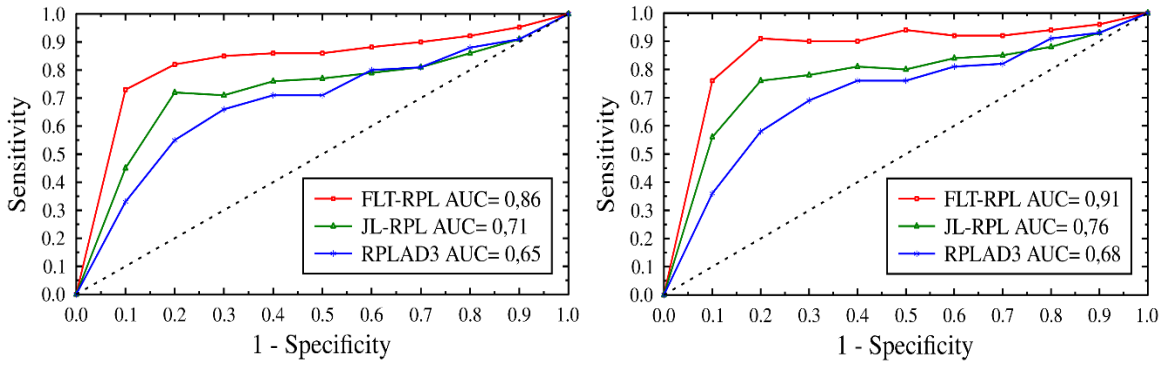
amount of energy expended to assess the behavior of the nodes concerning packet forwarding, as malicious nodes tend to consume less power than others. RPLAD3 obtains the poorest results due to its strategy, which requires a node to base its decisions regarding its neighbors solely on the behavior they exhibit toward a special packet that has been sent to them. This contributes to an increase in the number of false positives, particularly concerning the SFA-V variant, where malicious nodes can dynamically adjust their transfer rates based on the state of the network.

Figure 2-b) presents the results related to the evaluation of the sensitivity of the decisions made. It can be noted that these results corroborate those regarding precision. The shortcomings of JL-RPL and RPLAD3 mentioned earlier contribute to an increase in the false negative rates.



a) *b)*

Figure 2- Precision and Sensitivity of decisions made regarding the 5 variants in networks with 100 nodes: a) Precision ; b) Sensitivity.



a) *b)*

Figure 3- ROC curves of the decisions made regarding the SFA-V variant: a) fornetworks with 10 nodes; b) for networks with 100 nodes.

Figures 3-a) and 3-b) present the results of comparing the false positive rates to those of true positives for networks of 10 and 100 nodes, respectively, about the SFA-V variant. These ROC curves allow for a more detailed analysis of the ability of the three evaluated protocols to distinguish between malicious nodes and normal nodes through the AUC (Area Under the Curve) indicator. It is observed that for both types of networks, all three protocols achieve AUC values greater than 0.5, indicating that their decisions are not made randomly. However, in the 10-node networks, FLT-RPL achieves the highest AUC, with differences of 17.44% and 24.42% compared to JL-RPL and RPLAD3, respectively. In the 100-node networks, the AUC of FLT-RPL rises to 0.91, which represents differences of 16.48% and 25.27% compared to the other two protocols.

These results are attributed to FLT-RPL's ability to make decisions based not only on undelivered packets but also on residual energy and delivery latency. This capability increases with the number of nodes, as a higher density allows decisions regarding a malicious node to leverageinput from multiple neighbors. The strategy based onthe Dempster-Shafer theory reduces uncertainty in the decisions made.

Delay

To evaluate the latency of the three protocols in detecting a malicious node, we randomly deployed 10 networks under the conditions described in Section 4.1. The experiment ended as soon as a True Positive was detected. Each experiment was repeated 35 times. After each experiment, the elapsed time was measured. The averages of these values were calculated for each type of experiment, with a 95% confidence interval.

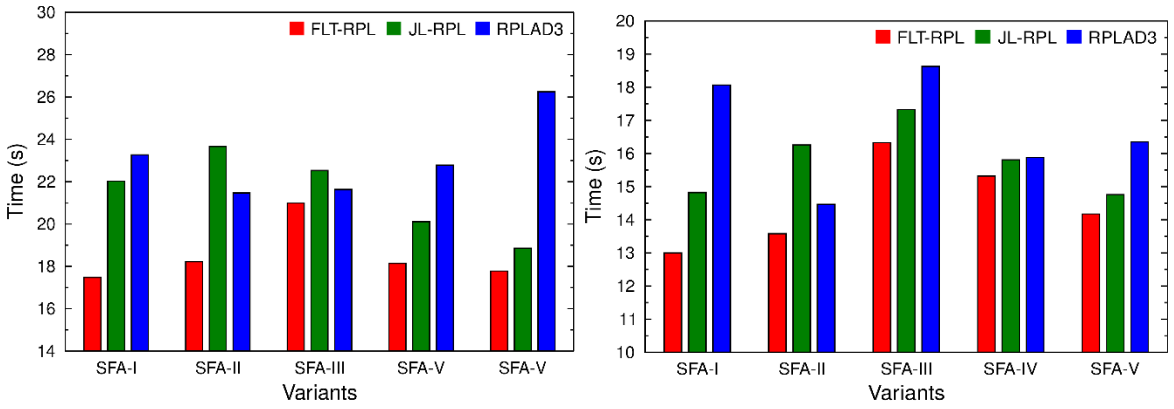


Figure 4- Delay in decisions made regarding the 5 variants: a) fornetworkswith 10 nodes ; b) fornetworks with 100 nodes.

Figures 4-a) and 4-b) show the results of evaluating the latency of the three protocols in their decision-making regarding each of the 5 variants of SFA for networks of 10 and 100 nodes. It is noted that FLT-RPL enables the fastest decisions. This is due to the strategies adopted by the JL-RPL and RPLAD3 protocols. Specifically, JL-RPL is executed periodically by a central node, namely the gateway, following a procedure that first involves suspecting nodes by adding them to a blacklist and then definitively declaring them malicious or not. RPLAD3 even employs a so-called punishment and forgetting process in its decision-making. These additional steps delay decisions, especially concerning the SFA-V variant, which itself aims to delay the delivery of packets.

In contrast to these two protocols, FLT-RPL utilizes a completely distributed strategy, allowing each node to check the behavior of its upstream neighbors (i.e., its parents on the DODAG) and downstream neighbors (i.e., its children). The resolution of the maximum flow problem enables rapid prediction of malicious behaviors, particularly based on energy expenditures. Any input from other nodes is only considered if they have evaluated the same suspect within the same time frame. This approach helps reduce latency in decision-making, especially when the network is sparse.

Energy efficiency

Figures 5-a) and 5-b) present the results of evaluating the energy expenditures of the three protocols during their decision-making regarding each of the 5 variants of SFA, with the context being networks of 10 and 100 nodes. Sending and receiving messages are the primary energy-consuming activities, making this an indirect evaluation of the message complexity of each protocol.

One can note that regardless of the type of network, FLT-RPL enables the most energy-efficient decisions. This is also attributed to the node suspicion strategies adopted by the JL-RPL and RPLAD3 protocols. Specifically, these strategies incur a protocol overhead manifested through the use of additional messages for updating the blacklists. Moreover, in JL-RPL, the detection of each malicious node by the central node leads to network flooding. In contrast, with FLT-RPL, only the children of malicious nodes are informed through a localized process within the two-hop neighborhood of the inquiring node.

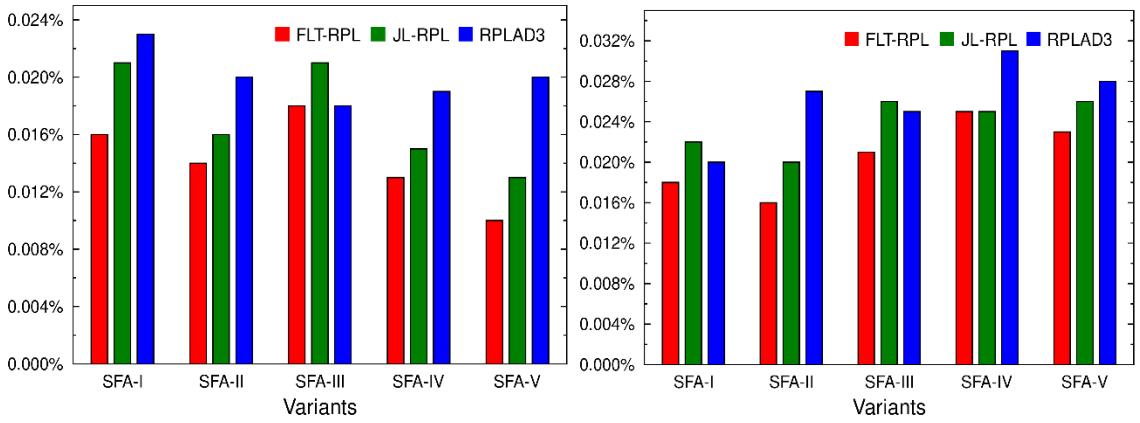


Figure 5- Energy waste ratios after the first decision regarding the 5 variants: a) for networks with 10 nodes ; b) for networks with 100 nodes.

CONCLUSION

In this study, we addressed the problem of detecting and neutralizing a malicious node perpetrating a selective forwarding attack in an IoT network based on the RPL protocol. We formulated this issue as a maximum flow problem, particularly for the process of calculating the trust level of nodes. We proposed a fully distributed strategy that relies on the number of lost packets, residual energy, and latency in packet delivery to detect suspicious behaviors. In cases of doubt or multiple opinions, a process based on the Dempster-Shafer theory is used to establish the final status of a suspected node.

The resulting protocol, called FLT-RPL, can be applied to all known variants of this type of attack while minimizing error rates, and it is also scalable, fast, and energy-efficient. FLT-RPL outperforms other major similar solutions recently proposed in the literature.

As part of future work, we plan to extend this solution to apply it to other topology-oriented attacks commonly faced by the RPL protocol, such as rank attacks, sinkhole attacks, replay attacks, and blackhole attacks.

ETHICAL DECLARATION

Conflict of interest: None. **Financing:** None. **Peer review:** Double anonymous peer review.

REFERENCES

[1] A. A. Bahashwan, M. Anbar, N. Abdullah, T. Al-Hadhrami, and S. M. Hanshi, “Review on common IoT communication technologies for both long-range network (LPWAN) and short-range network,” in Advances on Smart and Soft Computing. Springer Singapore, oct 2020, pp. 341–353.

[2] R. Kumar and R. Sharma, “Leveraging blockchain for ensuring trust in IoT : A survey,” Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 10, pp. 8599–8622, nov 2022.

[3] K. Avila, D. Jabba, and J. Gomez, “Security aspects for rpl-based protocols: A systematic review in IoT,” Applied Sciences, vol. 10, no. 18, p. 6472, sep 2020.

[4] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, “A review on the security of IoT networks : From network layer’s perspective,” IEEE Access, vol. 11, pp. 71 073–71 087, 2023.

[5] I. S. Alsukayti and M. Alreshoodi, “RPL-based IoT networks under simple and complex routing security attacks: An experimental study,” Applied Sciences, vol. 13, no. 8, p. 4878, apr 2023.

[6] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, “A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6lowpan of internet of things,” Sensors, vol. 22, no. 9, p. 3400, apr 2022.

[7] A. Verma and V. Ranga, “Security of RPL based 6lowpan networks in the internet of things: A review,” IEEE Sensors Journal, vol. 20, no. 11, pp. 5666–5690, jun 2020.

[8] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, “Intrusion detection systems in the internet of things: A comprehensive investigation,” Computer Networks, vol. 160, pp. 165–191, sep 2019.

[9] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, “Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications,” Sensors, vol. 21, no. 11, p. 3654, may 2021.

[10] J. Jiang and Y. Liu, “Secure iot routing: Selective forwarding attacks and trust-based defenses in rpl network,” Jan. 2022.

[11] N. Sinha and A. K. Mishra, “Metric-oriented comparison of selective forwarding attack detection techniques in IoT-based systems,” in Lecture Notes in Networks and Systems. Springer Nature Singapore, pp. 163–173, 2023.

[12] B. Shayesteh, V. Hakami, and A. Akbari, “A trust management scheme for IoT-enabled environmental health/accessibility monitoring services,” International Journal of Information Security, vol. 19, no. 1, pp. 93–110, jun 2019.

[13] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, “A comprehensive review on secure routing in internet of things: Mitigation methods and trust-based approaches,” IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4186–4210, mar 2021.

[14] J. Guo and I.-R. Chen, “A classification of trust computation models for service-oriented internet of things systems,” in 2015 IEEE International Conference on Services Computing. IEEE, jun 2015.

[15] M. Aaqib, A. Ali, L. Chen, and O. Nibouche, “IoT trust and reputation: a survey and taxonomy,” Journal of Cloud Computing, vol. 12, no. 1, mar 2023.

[16] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, “A survey on trust models in heterogeneous networks,” IEEE Communications Surveys &amp Tutorials, vol. 24, no. 4, pp. 2127–2162, 2022.

[17] A. Patel and D. Jinwala, “A reputation-based rpl protocol to detect selective forwarding attack in internet of things,” International Journal of Communication Systems, vol. 35, no. 1, oct 2021.

[18] E. G. Ribera, B. M. Alvarez, C. Samuel, P. P. Ioulianou, and V. G. Vassilakis, “An intrusion detection system

for RPL-based IoT networks," Electronics, vol. 11, no. 23, p. 4041, dec 2022.

[19] O. Yaman, B. Sokat, T. Ayav, and Y. M. Erten, "A novel countermeasure for selective forwarding attacks in iot networks," in 2022 3rd International Informatics and Software Engineering Conference (IISEC). IEEE, dec 2022.

[20] Z. Alansari, N. B. Anuar, A. Kamsin, and M. R. Belgaum, "RPLAD3: anomaly detection of blackhole, grayhole, and selective forwarding attacks in wireless sensor network-based internet of things," PeerJ Computer Science, vol. 9, p. e1309, mar 2023.

[21] O. Cruz-Mejía and A. N. Letchford, "A survey on exact algorithms for the maximum flow and minimum-cost flow problems," Networks, vol. 82, no. 2, pp. 167–176, jun 2023.

[22] N. Wang and D. Wei, "An adaptive Dempster-Shafer theory of evidence based trust model in multiagent systems," Applied Sciences, vol. 12, no. 15, p. 7633, jul 2022.

[23] R. Li, Z. Chen, H. Li, and Y. Tang, "A new distance-based total uncertainty measure in dempster-shafer evidence theory," Applied Intelligence, vol. 52, no. 2, pp. 1209–1237, may 2021.

[24] Contiki official homepage: http://www.contiki-os.org (dernier accès Juin 2023).